HSSEDI

Homeland Security Systems Engineering & Development Institute™

Prepared for:
Department of Homeland Security

Software Requirements Specification (SRS) for the United States Border Patrol (USBP) Integrated Surveillance Towers (IST) Common Operating Picture (COP)

30 August, 2019

Unclassified

Version 01-00

Homeland Security

This document is a product of the Homeland Security Systems Engineering and Development Institute (HSSEDI™).

Homeland Security Systems Engineering & Development Institute

The Homeland Security Systems Engineering & Development Institute (HSSEDI) is a federally funded research and development center (FFRDC) established by the Secretary of Homeland Security under Section 305 of the Homeland Security Act of 2002. The MITRE Corporation operates HSSEDI under the Department of Homeland Security (DHS) contract number HSHQDC-14-D-00006.

HSSEDI's mission is to assist the Secretary of Homeland Security, the Under Secretary for Science and Technology, and the DHS operating elements in addressing national homeland security system development issues where technical and systems engineering expertise is required. HSSEDI also consults with other government agencies, nongovernmental organizations, institutions of higher education, and nonprofit organizations. HSSEDI delivers independent and objective analyses and advice to support systems development, decision making, alternative approaches, and new insight into significant acquisition issues. HSSEDI's research is undertaken by mutual consent with DHS and is organized by tasks.

This document presents the results of a USBP task conducted under HSBP1017J00470: Customs and Border Protection (CBP) Program Management & Technical Support. The purpose of the task is to develop requirements for the Integrated Surveillance Towers (IST) Common Operatinal Picture (COP) software to be used by USBP.

The information presented in this report does not necessarily reflect official DHS opinion or policy.

This document was prepared for authorized distribution only. It has not been approved for public release.

For more information about this publication contact:

Homeland Security Systems Engineering & Development Institute

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Email: HSSEDI_info@mitre.org

http://www.mitre.org/HSSEDI

Record of Changes

No.	Date	Reference	A=Add M=Modify D=Delete	Description of Change
00-01	28 June 2019	DRAFT		Draft Version for Initial Review
00-02	22 July 2019	DRAFT		Front Matter (s.1,2) fleshed out
00-03	12 August 2019	DRAFT		Comments Adjudicated and Incorporated
00-04	27 August	DRAFT		Section 2.2 Update & Section 3 Reorg
01-00	30 August	Initial Release		Delivery to USBP

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Table of Contents

1 Introduction

The United States Border Patrol (USBP) is tasked with responsibility of securing the nation's borders. To accomplish this task, USBP uses a mix of infrastructure, technology and personal to establish and maintain the effective control of the borders.

The October 2006 Secure Border Initiative (SBI) Mission Need Statement (MNS) identified a number of capability gaps in USBP's ability to execute its mission. To address those gaps, the Arizona Border Surveillance Technology Plan identified a number of technologies to be deployed in accordance with local operational needs and constraints. Two key systems that implemented key technology recommendations were:

- Integrated Fixed Towers (IFT)
- Remote Video Surveillance System Upgrade (RVSSU)

These systems provide long range persistent surveillance to enable USBP personnel to detect, track, identify and classify illegal entries on our southern border through a series of integrated sensors and a common operating picture (COP). A pair of similar systems was implemented along the northern border:

- Northern Border Remote Video Surveillance System (NB-RVSS) and Maritime Detection Program (MDP) (this document treats these as one for COP purposes)

All of these systems employed different sensor packages, different software systems, and were implemented by different vendors. This resulted in three different COPs, three separate sustainment activities, and the need to interact with three different vendors when new capabilities were desired.

In 2018, the USBP Program Management Office Directorate (PMOD) considered shifting its approach to view these as a family of systems that could deploy towers with specialized instrumentation appropriate for their location while sharing an integrated COP. In this view, there are:

- Integrated surveillance towers that combine the Tower, Power, Instrumentation, and Communications (TPIC) capabilities. There could be several tower variants with instrumentation and capability appropriate to whatever section of the border they are intended to monitor.
- An Integrated Surveillance Tower (IST) Common Operational Picture (COP) that includes the command and control (C2) capabilities for the towers and their instrumentation. There would be a single COP for all USBP sectors and stations, though there may be many system instances.
- An Enterprise Network Operations Center, Security Operations Center, and Service Desk (NOC/SOC/SD) that provides network monitoring, security monitoring, and general help desk capabilities to the entire set of systems.

PMOD is developing a Joint Functional Requirements Document (JFRD) that combines the operational requirements of IFT, RVSSU and NB-RVSS/MDP programs. This JFRD is intended to support the acquisition of TPIC, IST COP, and NOC/SOC/SD capabilities through a common contract.

PMOD had also recognized that in addition to the vendors who have implemented its existing IFT, RVSSU, and NB-RVSS/MDP capabilities, there are other government entities who have implemented and fielded similar solutions. Demonstrations of these other IST COP software systems from government entities, like the Army and the Navy, are scheduled with the expectation that they will inform the process of procuring a system.

1.1 Purpose

A functional requirement document is intended to describe the capabilities and functions to be performed by a system, at a level of detail that is meaningful and understandable to an operational user. A Software Requirements Specification (SRS) is intended to describe those same functions and capabilities in a way that accounts for architectural and technical constraints and is meaningful to both an implementer and a tester. To do this, the SRS needs to derive requirements that account for technical realities and decompose functional requirements into elements that can be distinctly tested or demonstrated.

The purpose of this SRS and the architecture developed in conjunction with it is fourfold, listed in chronological order of when it may be applied:

1. To support the development of independent cost estimates by providing more detailed insights into the work that will be required.
2. To support technology demonstrations by helping both the demonstrating organizations and the technical evaluators to better understand the Border Patrol's requirements at a technical level.
3. To help an implementer understand and estimate the customizations that may be needed to their systems to meet the needs of the programs.
4. To help a tester create specific test cases and methods to ensure an implementer's system is acceptable once delivered.

1.2 Scope

This SRS has a very specific scope. It addresses the IST COP capabilities, including the Sensor command and control (C2). This SRS does not address the TPIC capabilities. It also does not address the Enterpise Network Operations Center, Security Operations Center, and Service Desk (NOC/SOC/SD) capabilities.

In addition, the current iteration of this document is focused solely on the software aspects of the IST COP. This document currently does not attempt to address requirements for the hardware on which the IST COP will be implemented. There are no hardware-related requirements for user workstations, display wall monitors, servers, storage, or the underlying network, all of which must be procured and set in place in the appropriate facilities.

The scope is focused on the IST COP system because the government intends to procure this separately from the TPIC and Enterprise NOC/SOC/SD capabilities. The scope is limited to software because a common set of software requirements are the most important part of making three different systems common, and there was no initial intent to constrain an implementer's choice of hardware. However, the procurement of an IST COP would need to include the hardware on which that system must run – and it can be appropriate to address hardware constraints in a software requirements specification – so it is possible future iterations of this document could expand in scope.

Note that the vision for the IST COP is to integrate with many other systems in the future. Only those systems for which interfaces are currently required are mentioned in this SRS. However, the potential for integration beyond what is specified in this SRS is desired by the government.

1.3 References

This IST COP SRS derives its authority from a series of documents established for existing programs. These started with a *Secure Border Initiative Mission Needs Statement (MNS)* issued in 2006 and traces through multiple Operational Requirements Documents (ORDs). Most recently and directly, this SRS traces to the JFRD, which is in the process of being approved. Appendix C contains full references for these documents.

The requirements in this document also reference many specifications, standards, and handbooks. Full references for these documents are in Appendix D, with references embedded in the requirements contained in sections 3 and 4.

2 Overall Description

This SRS is defining requirements for the IST COP. This section provides a more detailed perspective of the IST COP – both to ensure relevant information that does not qualify as a requirement is presented, and to provide a more detailed overview. Software functions, user classes, and expected documentation are addressed, along with software design constraints and assumptions.

2.1 Product Perspective

Section 1 mentioned PMOD's vision of handling the TPIC, COP, and NOC/SOC/SD as separate components of an overall IST system of systems. The IST COP includes both the software and the computing hardware, including networks and peripherals, needed to run the software. The IST COP will be employed in appropriate sector and station command and control centers (C2CENs) around the nation. This SRS focuses on the software portion of IST COP.

To understand the IST COP software, it is helpful to have a perspective on the existing systems fielded by USBP under their current programs, including the elements that will be addressed under the TPIC and NOC/SOC/SD going forward. These systems are:

- IFT
- RVSSU
- NB-RVSS and MDP

Each of these system has different capabilities. However, there are some similarities between them all. Every station with one of these technologies has a video wall with several video monitors in the front of the operations center displaying system maps, sensor feeds, and sometimes external systems – like a facility's closed circuit television (CCTV) monitors – for all to see.

Every operator workstation includes multiple monitors, two or more displaying information from their COP system, and generally at least one (often several) displaying information from other systems. These other systems range from USBP tools running on DHS OneNet, like Intelligent Computer-Aided Detection (ICAD) and Tracking, Sign-cutting, and Modeling (TSM), to feeds from commercial providers of other systems, like Texas Department of Public Safety (DPS) drawbridge cameras or Canadian National railroad video feeds.

The goal of a single COP system is to support the different capabilities and configurations of all three existing system in a single, consistent user interface.

2.1.1 RVSSU System

The RVSSU towers are typically 60 to 80 feet tall, though they can range from 40 to 120 feet. They may be either fixed or mounted on trailers that allow the unit to be more easily relocated. They can be tied into the local power grid or have their own generators and backup power for use in more remote locations. They typically communicate back to the base station via a microwave link, though they may also use the microwave link to communicate with another RVSS tower to be used as a relay.

RVSSU operates on a closed, restricted network of its own, and the NOC/SOC capabilities are hosted and staffed at each installation, with a broad service desk capability hosted in Phoenix to provide around-the-clock support.

The RVSSU Sensor Suite consists of a collection of electro-optical and infrared (EO/IR) video cameras to support both day and night use, as well as a laser illuminator and spotlight mounted on a pan-tilt unit (PTU – essentially a gimbal) to provide directional control of the sensors. The typical configuration includes two sets of this instrumentation, though up to four suites of instrumentation can be mounted in different configurations. In urban areas, there is typically a loud hailer that can support audio communication mounted on an additional PTU.

The RVSSU COP is based on PureTech System's PurActiv software, which provides the underlying map, sensor management and control, sensor display, video detection, archiving and retrieval, and other capabilities. Note that the RVSSU sensor suite configurations do not include a radar, though PureTech licenses a module for PurActiv that does have the capability to support radar integration.

While operator workstations can be configured differently at different stations, a typical RVSSU workstation consists of four screens:

- A map screen displaying the underlying Area of Responsibility (AoR) with fixed sites labeled and items of interest (IoIs) displayed in near-real time

- A camera screen – generally with 1-6 camera windows on it being controlled by the operators to pan, tilt, or zoom in on objects of interest. Motion detected by the system within a camera's viewshed causes the camera window to flash red, with the moving object's track appearing as a red line in the window
- An External Interface screen, usually showing an ICAD system window, where text-based displays of unattended ground sensor (UGS) hits could be viewed
- A still-imagery screen showing pictures from Buckeye cameras

2.1.2 IFT System

The IFT towers are typically 80-100 feet tall and are not mobile. They can be tied into the local power grid or have their own generators and backup power for use in more remote locations. They typically communicate back to the base station via a microwave link, though they may also use the microwave link to communicate with another IFT tower to be used as a relay or be linked in through a fiber-optic connection when feasible.

IFT operates in its own essentially closed network, but it does have a gateway to external networks that allow NOC/SOC capabilities to be provided remotely.

The IFT Sensor Suite consists of four fixed radars, mounted at 90 degrees to each other, ensuring a 360 degree coverage zone, plus one set of EO/IR video cameras to support both day and night use, as well as a laser illuminator and spotlight mounted on a PTU to provide directional control of the sensors.

The IFT COP is based on Elbit Systems' proprietary TORC2H and Peregrine software components, which together provide the underlying map, sensor management and control, sensor display, video detection, archiving and retrieval, and other capabilities.

While operator workstations can be configured differently at different stations, a typical IFT workstation consists of two or more screens:

- A map screen displaying the underlying AoR with fixed sites labeled and radar hits displayed in near-real time
- A camera screen allowing the operator to pan, tilt, or zoom in on items of interest detected by the radar
- Supplemental screens, as described above for RVSSU, may also be present in some operator workstations.

2.1.3 NB-RVSS System

The NB-RVSS units may be mounted on towers that can be up to 120 feet tall that are not mobile, or mounted onto buildings. They are tied into the local power grid. They may communicate back to the base station via a microwave link, though they may also use the microwave link to communicate with another NB-RVSS tower to be used as a relay or be linked in through a fiber-optic connection when feasible.

NB-RVSS operates on its own but has a gateway to DHS OneNet, and Enterprise NOC/SOC/SD capabilities are hosted in a centralized location.

The NB-RVSS Sensor Suite consists of two pairs of electro-optical and infrared (EO/IR) video cameras to support both day and night use mounted on a PTU to provide directional control of the sensors. They typically do not include laser range finders or illuminators.

The MDP system consists of camera towers, radar towers, commercial radar data, maritime tracks from Automated Identification System (AIS), encrypted AIS (eAIS), and the National Oceanic and Atmospheric Administration (NOAA) Vessel Monitoring System (VMS), and a COP. MDP units employ the same mounting, communications, and sensor suites as NB-RVSS. MDP units use microwave links to relay data through other MDP units and then to an NB-RVSS unit for communication with the C2CEN. MDP radar towers are placed so as to provide overlapping coverage in a sector's AoR, and use microwave connectivity between them to share radar detections that are then processed by a processor collocated with one of the radar units to generate tracks. Tracks are transferred to the command center in the same way that video from MDP camera towers are transferred.

At northern border C2CENs, one COP integrates video feeds and controls from NB-RVSS and MDP camera towers, and provides a fused data display for radar tracks from MDP radar towers and commercial sources of radar tracks, AIS, eAIS, and NOAA VMS. The northern border COP is based on the Navy's Sensor Management System/Joint Perimeter Surveillance Command and Control (SMS/JPSC2) system, which provides a foundation for integrating different components as well as much of underlying map, sensor management and control, and sensor display capabilities, while linking in third party archiving and retrieval software and including a rudimentary interface to TSM.

NB-RVSS workstations ranged from two to eight screens:

- A map screen displaying the underlying AoR with fixed sites labeled and radar hits and tracks displayed in near-real time and alerts details displayed in a window.
- An External Interface screen with a TSM interface open, tracks pushed over to TSM could be edited. This could include an ICAD screen – or other tools on DHS OneNet – as well.
- Sometimes, a camera screen – generally with one to six camera windows on it being controlled by the operators to pan, tilt, or zoom in on objects of interest.
- Other screens, ranging from dispatch status, to still-imagery from ICAD-4, to external system feeds from railroad video cameras.

In addition to the COP interface on workstations in the C2CEN, northern border stations with NB-RVSS/MDP have begun piloting integration with a JPSC2 interface on mobile notebooks carried by USBP agents in the field. Mobile notebooks connect to SMS/JPSC2 over commercial cellular networks. Mobile operators can view the same radar tracks as JPSC2 users in the C2CEN, can add information to the JPSC2 COP that is shared with C2CEN users, and are planned to have access to video from NB-RVSS and MDP camera towers in the near future.

2.2 Product Functions

The IST COP will perform many functions. These functions can be grouped together and described in several different ways. This SRS organizes product function into the following categories:

- **System Administration**. The management of back-end system functions and the user interfaces related to them. This set of functions underpins and enables the mission areas supported by the system.
- **Sensor and Interface Management**. The setup, configuration, and management of data related to sensor and external system interfaces. As with system administration, this set of functions underpins and enables the mission areas supported by the system.
- **Map Interactions**. The interactions between a user, the system's map, and the elements displayed on the map, including IoIs. This set of functions supports the user's ability to predict, detect, track, and respond.
- **Sensor Interactions**. The interactions between a user and specific sensor displays, which includes controlling the sensors and viewing their output. This set of functions supports the user's ability to detect, identify, classify, and track.
- **Automated Capabilities**. The back-end functions that perform the motion detection, IoI identification and classification, mult-sensor correlation, pattern detection, and other analytics. This set of functions supports the user's ability to predict, detect, identify, and classify.
- **Data Storage and Retrieval**. The storage of sensor data, metadata, and any other relevant data, as well as the ability to search, retrieve, annotate and export data. This set of functions primarily supports the user's ability to report on and resolve events.

A notional functional architecture was produced to help decompose the elements of a COP system. Appendix E more thoroughly describes this architecture, but it is illustrated at the top level in Figure 1, below.

The notional architecture groups functions into six sets of services:

1. Common Display Services. These services exist largely behind the scenes to ensure maps and other information will be displayed properly. Management of these back-end services would fall within the System Administration category above.
2. User Interaction Services. These services support the user interactions with the system and are spread across every category listed above, with a significant focus within the map interactions and sensor interactions categories.
3. Detection and Tracking Services. These services provide motion detection and tracking and fall within the Automated Capabilities category above.

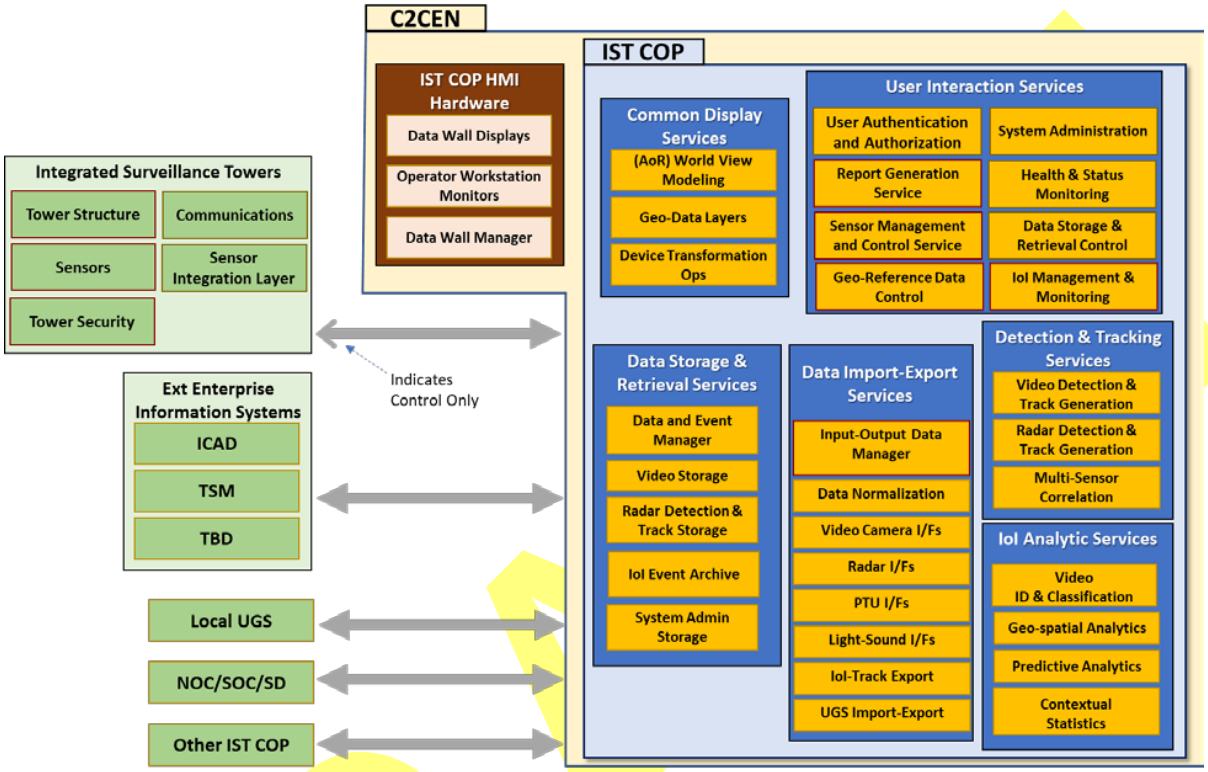

Figure 1 – IST COP Notional Functional Architecture

4. IoI Analytic Services. These services provide the identification, classification, and other analytic services, which fall within the Automated Capabilities category above.
5. Data Import-Export Services. These services provide the necessary translations and other interactions with external sensors and systems, and they fall within the sensor and interface management category above.
6. Data Storage and Retrieval Services. These services provide the capability to interact with the elements of a data management system – databases or filesystems – and they fall within the Data Storage and Retrieval category above.

The elements of the architecture diagram outside of the IST COP are not in scope for this document.

2.3 User Classes and Characteristics

System access in the COP software will be assigned by roles, and roles will be assigned to individual users. System functions and interfaces will be associated with these roles. The roles inferred from observations in the field are:

- Operators. These are the standard users of the system who are sitting in front of workstations monitoring sensor feeds, controlling sensors, finding IoIs and following up on system-identified IoIs. These users should have full access to map and sensor

capabilities and can search and review archived data if needed, without the capability to export data. These users do not need access to any special functions or system administration capabilities. Operators are not always USBP personnel; on the southern border there were National Guardsmen serving as operators to supplement the Border Patrol. Where operators are USBP personnel, there can be a broad range of job designations ranging from agents to law enforcement communication assistants and law enforcement information system specialists.

- Supervisors. These are users who oversee the operators and can perform the same functions as an operator if needed. These users also need to be able to create and export video clips, still imagery, and other archived sensor data to document incidents that occur, and they may need the ability to review certain logs.
- System Administrators. These are the users who set up, configure, or reconfigure the system. They need access to all system configuration parameters and logs. They will generally have access to all functions that can be accessed by the operator or supervisor as well. These users may not be stationed with other operators and will need to be able to access the system remotely.
- NOC/SOC/SD Operators. These users perform many system administration functions but may be separate from system administrators and require their own roles. Service Desk users, in particular, need to be able to see what an operator or supervisor is seeing in order to fully understand a problem. These users may not be stationed with operators and will need to be able to access the system remotely.

The software will allow system administrators to define roles and associate roles with system functions, so stations with responsibilities that differ from the above can define their roles as needed. For example, if a station wanted to define a role for field service engineers that allowed them to setup and configure sensors in the COP system without having access to other operator or system administration functions, this system will support it. This flexibility is also needed to support potential future changes to mission or staff that cannot be predicted at this time.

In addition, most modern systems run processes in the background, and these processes will need to be associated with headless accounts – ones that are not associated with a specific individual. Headless accounts still need to have permissions and roles assigned so they can accomplish what they need to without having access to do more than they need.

2.4 User Documentation

There is an expectation that the capabilities and functions of the system will be well documented. At a minimum, there should be documentation to support:

- Training. This can be any combination of documents, slides, or audio-visual presentations. Training documentation should be available to a user online within the system as a reference.

- User Reference. Documentation with supporting graphics describing the system's capabilities and functions for all classes of users should be available to users online within the system as reference material.
- System Administration. This would include installation documentation, troubleshooting procedures, and version description documents.
- Third-party Capability Integration. Documentation sufficient to allow a third party developer to understand whether they can integrate a particular capability with the system and if so, how. This could take the form of Interface Control Documents (ICDs) or something else.
- Third-party Sustainment. A combination of design documentation and inline code comments to ensure the system's code line is understandable to a third party.

2.5 Design and Implementation Constraints

The Border Patrol has a vision for what they want from IST, which includes the COP system. In addition to separating the TPIC from the COP system and having an Enterprise NOC/SOC/SD, there is a recognition that there are external entities collecting sensor data that is useful to the border agent's mission and that there are necessary integrations to other USBP systems. There is also a vision (not yet a requirement) of moving towards an agent-less operations center, which would allow the border patrol agents in the field to request information from the COP system and get the situational awareness they need on their own handheld devices.

Constraints on the Design and Implementation of the IST COP include:

1. The system cannot run on a closed, restricted network. There will need to be interfaces to DHS OneNet and to systems and information sources outside of that as well.
2. The system needs to be architected and designed such that third-party capabilities can be identified in the future and then quickly and cost-effectively integrated after the initial delivery of the COP system.
3. The system will need to be accreditable by DHS.
4. The system will need to be able to quickly and cost-effectively react to changes in sensor packages over time, including the ability to receive, decode, analyze, display, and otherwise handle increases in resolution from video sensors.
5. The system may need to integrate with existing tower infrastructure and sensor packages from all three legacy programs: IFT, RVSSU, and NB-RVSS/MDP. The design will need to support this possibility.
6. The system will need to ensure a single instance of the system is able to support new TPIC installation in AoRs that also have legacy towers and sensor packages.
7. The COP system will need to be able to scale to have a single instance of the system support up to 37 towers (296 video feeds, 111 PTUs, and as many as 13 operator workstations).

8. Existing facilities, furniture, and computing hardware in C2CENs should be reused where feasible.

2.6 Assumptions and Dependencies

The initial operational requirements documents (ORDs), and FRDs were written for single, integrated systems. By splitting the TPIC and COP systems, there are requirements that could be performed by either or need to be allocated between the two.

In addition, the Border Patrol's vision for how to implement these capabilities has evolved since the development of the ORDs, and the appropriate decomposition of requirements from the ORD through the JFRD into this SRS need to account for this current vision.

The key assumptions for the IST COP are:

1. Performance requirements involving both the TPIC and COP systems will be allocated evenly to both the TPIC and the IST COP.
2. Video encoding will be done by the TPIC, regardless of whether it is implemented in hardware or software.
3. The COP system will be required to correlate/fuse data into tracks, as well as accept already fused data from the TPIC. The TPIC system may move towards integrating motion detection and track generation from video cameras or other sensors to the edge and providing complete tracks to the COP, but the COP cannot rely on this being done and will retain a requirement to provide this capability.
4. The COP system will not initially be required to integrate with any border agent dispatch systems. The dispatching of agents will remain separate.
5. The COP system will not initially be required to be operated on a border agent's mobile device or other very small screen, which could require the development of substantially different user interfaces.
6. The COP system should be able to ingest external video feeds to support the potential integration of existing capabilities (e.g., aerostats) or capabilities currently being examined that could some during this systems usefule life (e.g., agent-launched drones).
7. The COP system does not have to implement Section 508 accessibility requirements.

These assumptions have been used to help shape the degree to which requirements not explicitly stated in the JFRD have been decomposed, either limiting or motivating how additional detailed requirements have been derived.

3 Functional Requirements

This section addresses the requirements that address the behavior of the system. When used in this section, the terms "system" or "the system" refer to the IST COP system.

3.1 System Administration

This section addresses general setup and maintenance features underpinning the use of the system.

3.1.1 Geospatial Data

This section addresses geospatial database management. The USBP vision is that the system will get its map data and updates from Enterprise Geospatial Information Services (eGIS). There is an expectation that map files will include labeled features (e.g., roads, rivers, and lakes).

3.1.1.1. The system shall translate geodetic information input into the system to a common geodetic reference system, as defined by the World Geodetic System of 1984 standard.

3.1.1.2. The system shall allow system administrators to load map files.

3.1.1.3. The system shall allow system administrators to update map files.

3.1.1.4. The system shall support map files with resolutions ranging from 100 x 100 pixels per 100 foot by 100 foot area to 100 x 100 pixels per 25 mile by 25 mile area.

3.1.1.5. The system shall support linkages between map files of different resolutions to provide the ability to zoom in and zoom out.

3.1.1.6. The system shall allow operators and supervisors to create map overlays consisting of icons, text, and drawn polygons associated with geodetic coordinates.

3.1.1.7. The system shall adhere to MIL-STD-2525B for relevant symbology.

3.1.1.8. The system shall allow operators and supervisors to export map overlays in Keyhole markup language (KML) format.

3.1.1.9. The system shall allow operators and supervisors to import map overlays stored as KML files.

3.1.1.10. The system shall make all overlays in a system instance available to all users.

3.1.2 Identity and Access Management

This section addresses the management of user identities, authentication of those identities, and authorization of users to specific system functions. The vision is to use DHS PIV cards where possible, with password-based access as a backup, leveraging USBP Active Directory instances.

3.1.2.1. The system shall enforce the use of a distinct user name for each user account.

3.1.2.2. The system shall be capable of using Microsoft's Active Directory as the primary source for user identities.

3.1.2.3. The system shall ensure each user account is assigned exactly one role, either that of operator, supervisor, system administrator, or NOC/SOC/SD operator.

3.1.2.4. The system shall ensure user identities are associated with a strong password, as defined in DHS 4300A *(details below as written in v12, section 5.1.1.1)*

a) Passwords shall be at least 12 characters in length

b) Passwords shall not contain a dictionary word

c) Passwords shall not contain proper nouns

d) Passwords shall not be the same as the user ID

e) Passwords shall not contain any information that could be readily guessed about the creator of the password, to include employee serial number, Social Security number, birth date, or phone number

f) Passwords shall not be the same as any of the user's previous 8 passwords

g) Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123

h) Passwords shall not contain word, noun, or name spelled backwards or with a single digit appended, or with a two-digit "year" string

3.1.2.5. The system shall ensure passwords expire in distinct timeframes

a) The system shall support the configuring of expiration timeframes

b) The system shall default the password expiration timeframe to 90 days

c) The system shall limit access to the expiration timeframe to system administrators

3.1.2.6. The system shall not allow a user with an expired password to log in until that password has been changed

3.1.2.7. The system shall not allow a user with no defined password to log in until a password has been set

3.1.2.8. The system shall provide a capability for a user to set or change their password

a) A password change capability shall be able to be initiated by the user

b) A password change capability shall be able to be initiated by the system

c) A password change capability shall require the user to successfully enter their current (expired or unexpired) password if a current password exists

d) A password change capability shall require the user to successfully enter a new password that conforms to strong password requirements

e) A password change capability shall force the user to validate the entry of a new password (typically done by having them enter it a second time and comparing the two)

3.1.2.9. The system shall ensure user identities are associated with DHS Personal Identification Verification (PIV) token certificates

3.1.2.10. The system shall not store passwords, biometrics, or PIV token certificates in clear text in any sort of database or file.

3.1.2.11. The system shall ensure only one user can be logged into a workstation at any given time.

3.1.2.12. When no user is logged into a workstation, the system shall display a login screen

a) The login screen shall include enterable user identify and password fields

b) The login screen shall support the use of a PIV card and the enterable Personal Identification Number (PIN) field

c) The system login screen shall display a warning banner, as specified and provided by the appropriate DHS Chief Information Security Officer (CISO)

3.1.2.13. The system shall mask passwords to ensure they cannot be seen by users

3.1.2.14. The system shall mask PIV card PINs to ensure they cannot be seen users

3.1.2.15. The system shall ensure users who fail to enter a password or PIV card PIN more than a specified number of times will be locked out of the system

a) The system shall support configuring a parameter defining the number of invalid password entries needed to lockout a user

b) The system shall support configuring a parameter defining the number of invalid PIV card PIN entries needed to lockout a user

c) The system shall support configurating a parameter defining how long a user will be locked out after entering incorrect passwords or PIV card PINs more than the specified number of times

3.1.2.16. The system shall provide a capability to unlock a user account to allow that user to attempt to login to the system again prior to the defined lockout period ending

3.1.3 System Logs

This section addresses setup and management of system logs. How many log files exist and other details of implementation are left to the system provider. However, the vision is that most logs are for system adminsitrators but that there will be an operations log that operators can access and contribute to as well.

3.1.3.1. The system shall automatically log the following events in system log files:

a) User logins, logouts, and unsuccessful attempts to log in

b) Changes to user account names, passwords, and assigned roles

c) Each time a user takes and releases control of a sensor
d) Additions and modifications to map files
e) The use of data export functions
f) Commands performed by system administrators and headless accounts
g) Any elevation of system privileges
h) A user's clicks and the context (screen) they were in to support analysis of system usage

3.1.3.2. The system shall record the following information with each event written to system log files:
a) A human-readable name describing the event
b) The date of the event in YYYYMMDD format
c) The time of the event in HHMMSS format referenced to coordinated universal time (UTC)
d) The username of the account performing the event
e) The Internet Protocol address of the system that originated the event
f) The identification number of the sensor for which control was taken or released (for sensor control events)
g) The full file path and file name of map files loaded, map files modified, and experted files created (for map loading, map modification, and export function events)

3.1.3.3. The system shall ensure all components of a system instance have their clocks synchronized within one second to ensure accurate times are written to system log files

3.1.3.4. The system shall write system log files to a location configured by a system administrator

3.1.3.5. The system shall include a description of the contents of the log files and date-time range of events logged in the file in the names of system log files

3.1.3.6. The system shall retain system log files for not less than 28 days

3.1.3.7. The system shall provide access to system log files only to authorized users

3.1.3.8. The system shall not allow any users to edit system log files

3.1.3.9. The system shall include a separate operations log that can be accessed by all users

3.1.3.10. The system shall allow a user to create and name an event in the operations log

3.1.3.11. The system shall allow a user to include one or more screenshots from any screen in the system, including sensor feeds, into the operations log

3.1.3.12. The system shall allow a user to associate a file with an operations log entry

3.1.3.13. The system shall allow a user to add text to an operations log entry

3.1.3.14. The system shall allow only authorized users to edit or delete operations log entries

3.1.4 NOC/SOC/SD

This section addresses interfaces with a NOC/SOC/SD without including the specific requirements associated with network management, security management, or service desk operations.

3.1.4.1. The system shall support the ability of a user to login remotely

3.1.4.2. The system shall support being installed in a remote facility while behaving as if it were part of a local installation

3.1.4.3. The system shall provide a user the capability to open a help desk ticket from within any screen

3.1.4.4. The system shall populate every help desk ticket it opens with the user's identity, the screen from which the ticket was opened, and a date/time stamp when it was opened

3.2 Sensor and Interface Management

This section addresses the setup and maintenance of parameters related to the configuration of sensors and other interfaces. The actual use and control of sensors will be done elsewhere in the system, and requirements for the use and control of sensors is described later in section 3.3.

3.2.1 Sensor Interfaces

This section addresses the setup and maintenance of parameters related to the configuration of sensors.

3.2.1.1. The system shall implement common user interfaces, referred to as "sensor interfaces," for each type of supported sensor

3.2.1.2. The sensor interfaces shall include the commands necessary to control each sensor

3.2.1.3. The sensor interfaces shall include the commands necessary to query and receive health and status information from each sensor

3.2.1.4. The sensor interfaces shall describe the sensor data and metadata needed to receive each sensor feed

3.2.1.5. Where the TPIC systems are capable of performing data correlation and fusion, the sensor interfaces shall include parameters needed by the system to make use of the correlated or fused data

3.2.1.6. The system shall store configuration settings for all sensors connected to it, including

a) Name, type, and description
b) The geospatial coordinates of that sensor's location
c) The minimum and maximum range of the sensor
d) For directional sensors, the azimuth, tilt, elevation, and any other attributes of the sensor needed to determine where a sensor is pointed
e) For directional sensors, the parameters that define the sensor's viewshed

f) For PTUs the minimum and maximum azimuth and elevation supported
g) For audio devices, the minimum and maximum volume levels
h) Network address, port, protocol, and any other settings needed to support communication with the sensor

3.2.1.7. The system shall allow a user to calibrate a sensor with a focal point by entering a known geocoordinate while pointing that sensor at a known location, calculating the difference between the detected focal point and the entered coordinate, and storing the calibration offset

3.2.1.8. The system shall apply calibration offsets in calculating geocoordinates associated with those specific sensors

3.2.1.9. The system shall allow a user to adjust sensitivity settings on radars, and other applicable sensors

3.2.1.10. The system shall automatically acquire configuration settings, health and status from sensors that are capable of dynamically providing that information

3.2.1.11. The system shall allow an authorized user to set values for any sensor configuration settings

3.2.2 ICAD Interface

This section addresses the setup and maintenance of parameters needed to interface with the ICAD system.

3.2.2.1 The system shall be able to receive information on UGS from the ICAD system

3.2.2.2 The system shall support the receipt and storage of UGS location and configuration data

3.2.2.3 The system shall support the receipt and display of UGS low battery warnings and any other published health and status data

3.2.2.4 The system shall support the receipt and display of UGS alerts, with all supporting information and metadata

3.2.2.5 The system shall support the receipt and display of still imagery associated with Buckeyes and other UGS-related cameras

3.2.2.6 The system shall automatically create an ICAD event entry when a TSM entry is created (see section 3.2.3).

3.2.3 Tracking, Sign-Cutting and Modeling (TSM) Interface

This section addresses the setup and maintenance of parameters needed to interface with the TSM system.

3.2.3.1 The system shall allow the operator to identify an event to become a TSM entry

a) The operator shall be able to identify an IoI as the basis of a TSM entry

b) The operator shall be able to identify a distinct track history as the basis of a TSM entry

c) The operator shall be able to identify an alert as the basis of a TSM entry

d) The operator shall be able to identify any screen in the system to have a screenshot of that screen be the basis of a TSM entry

3.2.3.2 The system shall automatically populate all relevant information from the system into the TSM entry

3.2.3.3 The system shall automatically attach a screenshot of the selected IoI, radar track, or screen into TSM associated with the entry

3.2.3.4 When using track history as the basis for a TSM entry, the system shall automatically create TSM sub-entries for each registered point along the track

3.2.3.5 The system shall require the operator to provide whatever additional information is necessary to create a valid TSM entry

3.2.3.6 The system shall allow the operator to provide additional notes or other information to the TSM entry

3.2.3.7 The system shall require the operator to take an action to actually create the TSM entry

3.2.3.8 The system shall receive and display a confirmation of successful TSM entry creation

3.2.3.9 The system shall receive and display an error messages associated with a failed attempt to create a TSM entry

3.2.4 Blue Force Tracking Interface

This section addresses the setup and maintenance of parameters needed to interface with a Blue Force Tracking system.

3.2.4.1 The system shall have the ability to receive information from the P25 Blue Force Tracking system

3.2.4.2 The system shall have the ability to receive information from any Blue Force Tracking system, as long as the interface is based on standards that are specified in advance

3.2.4.3 The system shall display the locations of blue force elements as part of the COP

3.2.4.4 The system shall display blue force elements using blue icons

3.2.4.5 The system shall display USBP agents, CBP Air and Marine Operations (AMO) assets, and other blue force elements using distinct icons for each

3.2.4.6 The system shall associate blue force elements with a map layer for which the display can be controlled by the operator

3.2.5 Federated C2 System

This section addresses interfaces allowing federation or similar cooperative interactions with other instances of the IST COP system.

3.2.5.1 The system shall be able to connect to separate C2 center installations at different facilities

3.2.5.2 The system shall support configuration to show or hide specific installations

3.2.5.3 The system shall provide visibility into what sensors and system components exist in other installations

3.2.5.4 The system shall allow an operator to transfer control of a sensor or system component to another installation

3.2.5.5 The system shall allow an operator to request control of a sensor or system component at another installation

3.2.5.6 The system shall alert operators at an installation when an operator at a different installation has requested control of a sensor or system component

3.2.5.7 The system shall allow an operator to grant or deny a request to control a sensor or system component from a different installation

3.2.5.8 The system shall allow an operator at a different installation to release their control of a sensor or system component

3.2.5.9 The system shall allow an operator to take back control of a sensor or system component that has been granted to an operator at a different installation

3.2.5.10 The system shall notify an operator at a different installation when a sensor or system component they had controlled is no longer in their control

3.2.5.11 The system shall log all actions related to requesting, granting, denying, releasing, or taking back control of a sensor of system component initiated or received by that system

3.2.5.12 The system shall allow an operator to designate a different installation as the fallback installation to support disaster recovery or continuity of government

3.2.5.13 The system shall provide the ability to associate all sensors and system components to the primary control of a different installation

3.2.5.14 The system shall provide the ability to re-associate all sensors and systems components back to the control of their original installation

3.2.5.15 The system shall limit access to the ability to associate or re-associate all sensors and system components to specified roles

3.3 Map Interactions

This section addresses the operational user interactions with the system.

3.3.1 Annotations and Layers

This section addresses map display, navigation, annotation, and tools.

3.3.1.1. The system shall support the display of different visual elements in different windows, including:
   a) Map and map layers
   b) Sensor feeds, including video
   c) Data archive and retrieval screens
   d) External systems
   e) System setup and administration screens

3.3.1.2. The system shall allow the operator to arrange windows among the screens at their workstation

3.3.1.3. The system shall allow the operator to save an arrangement of the screens at their workstation, along with any other personalization settings in the system and the user's identity, with a name provided by the operator (this is called a "preset")

3.3.1.4. The system shall automatically save the arrangement of screens at a workstation when an operator logs out

3.3.1.5. The system shall include all personalization settings associated with an operator when saving an arrangement of screens

3.3.1.6. When an operator logs in, the system shall set the arrangement of screens to what they were the last time that operator logged out

3.3.1.7. The system shall allow the operator to load a saved preset by providing the name or selecting from a list of saved preset names

3.3.1.8. The system shall load all personalization settings associated when loading a preset

3.3.1.9. The system shall support at least 600 preset arrangements of screens across all users within an installation

3.3.1.10. The system shall allow operators to edit the names of presets they had saved

3.3.1.11. The system shall allow operators or to delete presets they had saved

3.3.1.12. The system shall allow system adminsitrators to edit the names of or delete any saved preset

3.3.1.13. The system shall display a map of the AoR

3.3.1.14. The system shall allow the operator to zoom in and out on the map screen

3.3.1.15. The system shall allow the operator to scroll the map screen in any direction at its current zoom level

3.3.1.16. The system shall allow the operator to return to the full view of the AoR with a single command

3.3.1.17. The system shall display international boundary lines on the map

3.3.1.18. The system shall display road names on the map

3.3.1.19. The system shall display names for common geographical features on the map, including lakes, waterways, and mountains
3.3.1.20. The system shall display a compass rose on the map
3.3.1.21. The system shall allow the user to display or hide the compass rose
3.3.1.22. The system shall allow the user to select a point on the map with a cursor and choose to see the geocoordinates of that point
3.3.1.23. The system shall display towers, sensors, or other assets defined in the system on the map
3.3.1.24. The system shall use distinct icons to display each type of asset defined in the system
3.3.1.25. The system shall allow the user to define and name static objects on the map by selecting a point on the map with the cursor
3.3.1.26. The system shall allow the user to define and name objects on the map by providing coordinates
3.3.1.27. The system shall automatically associate geocoordinates with all user-defined objects
3.3.1.28. The system shall allow the user to associate descriptions with user-defined objects
3.3.1.29. The system shall allow the user to associate icons and colors with user-defined objects
3.3.1.30. The system shall allow the user to edit names, descriptions, icons, and colors associated with user-defined objects
3.3.1.31. The system shall provide a mechanism allowing the user to relocate a user-defined object on the map
3.3.1.32. The system shall allow the user to delete user-defined objects
3.3.1.33. The system shall ensure the icons and labels for all assets defined in the system and all user-defined objects scale appropriately when zooming in and out of the map
3.3.1.34. The system shall allow the user to define and name map layers
3.3.1.35. The system shall provide a map layer that includes all sensors configured in the system
3.3.1.36. The system shall include UGS for which information was received via the ICAD interface in the map layer with other configured sensors
3.3.1.37. The system shall allow the user to associate user-defined objects with map layers
3.3.1.38. The system shall allow the user to toggle the display of each map layer on or off individually
3.3.1.39. The system shall allow the user to edit the names of user-defined map layers
3.3.1.40. The system shall allow the user to delete user-defined map layers
3.3.1.41. The system shall retain all user-defined objects and their information when the map layers to which they were associated is renamed or deleted
3.3.1.42. The system shall retain deleted map layers for at least 24 hours in a state that can be restored by a system administrator

3.3.1.43. The system shall ensure all objects associated with visible map layers that remain in the on-screen area of the map continue to be seen as the user scrolls the map in any direction
3.3.1.44. The system shall allow the user to share their view of the map, including visible layers and all associated objects, with another system user
3.3.1.45. The system shall alert a user if another system user is trying to share their map
3.3.1.46. The system shall allow a user to set their system map, including layers and objects, to a shared view provided by another user
3.3.1.47. The system shall allow a user to clear the alert received when another user tries to share their map, without changing the map view to what another user is sharing
3.3.1.48. The system shall display Items of Interest (IoIs) on the map in a location that matches their currently detected geocoordinates
3.3.1.49. The system shall ensure the location of an IoI remains updated as the geocoordinates of an IoI change
3.3.1.50. The system shall allow a user to search the map and all active layers by entering a search string
3.3.1.51. The system shall display a list of all sensors, IoIs, and other objects whos identifiers contain the search string, if there is more than one result
3.3.1.52. The system shall allow the user to select a result from the list and then highlight that object on the map and center the map on its location
3.3.1.53. If there is only one result, the system will highlight the object whos identifier contained the search string and center the map on that object
3.3.1.54. The system will allow the user to dismiss the list of search results

3.3.2 Items of Interest (IoI)

This section addresses how users manually detect, identify, classify, and otherwise interact with IoIs, to include system alerts, track history, or other representations.

3.3.2.1. The system shall visually alert the operator when an object is detected that could be an IoI

3.3.2.2. The system shall enable the operator to visually determine whether a detected object is an IoI

3.3.2.3. The system shall enable the operator to identify whether a detected IoI is:

a) humans traveling alone on foot
b) a group of humans traveling on foot
c) humans traveling alone on animals
d) a group of humans traveling on animals
e) moving ground conveyance (e.g. ATVs, motorcycles, automobiles, or trucks)

f) moving or stationary water conveyances (e.g. Jet Skis, motor boats, sailboats, fishing boats and commercial watercraft)

g) air conveyance (e.g. low-flying drones or ultralight aircraft)

3.3.2.4. The system shall allow the operator to select an IoI on the map

3.3.2.5. The system shall allow the operator to classify an IoI by assigning a label, descriptive text, threat level, number in group (default 1), priority, and other notes (e.g. whether an assist was provided)

3.3.2.6. The system shall allow the operator to highlight an IoI by assigning a color to its icon

3.3.2.7. The system shall allow the operator to designate that a detected object is not an IoI

3.3.2.8. The system shall allow the operator to access the following for each IoI currently being tracked

a) Current Location (geocoordinates), Heading, and Speed

b) Visual Track History and Track Duration

c) Classification Labeling and Description

3.3.2.9. The system shall allow the operator to designate an IoI to be tracked by a specific sensor

3.3.2.10. The system shall allow the operator to designate an IoI to be tracked by any sensor in range

3.3.2.11. When the operator designates an IoI to be tracked by any sensor in range, the system shall select which sensor is most appropriate at any point in time

3.3.2.12. The system shall automatically slew the named or selected sensor to maintain the IoI within the sensor's field of view as the IoI moves within the surveillance area and maintains line of sight (LOS)

3.3.2.13. The system shall alert the operator when track of the IoI crosses the boundary of the tracking sensor’s field of view.

3.3.2.14. The system shall enable the operator to access a list of every IoI within the AoR

3.3.2.15. If the operator selects an IoI from the list of IoIs in the AoR, the system shall center the map on that IoI’s location and highlight it

3.3.2.16. The system shall maintain a single and continuous track of an IoI as the IoI transits overlapping Scanning Sensor surveillance areas within the AoR.

3.3.2.17. When an IoI splits into multiple IoIs, the system shall maintain and carryover the attributes associated with the original IoI into each of the newly created IoIs.

3.3.2.18. When a group of IoIs merge into a single group, the system shall attempt to maintain the individual IoIs and retain all attributes assigned to each of them

3.3.2.19. When a group of IoIs merge into a single group, the system shall allow an operator to highlight the group on the map and designate them to be a single IoI

3.3.3 Sensor Health and Status

This section addresses visibility and handling of sensor health and other status information.

3.3.3.1. The system shall track the operational status of each sensor and system component with which the operators can interact as defined in the ICD

3.3.3.2. The system shall allow the user to query the operational status of any sensor or system component

3.3.3.3. The system shall allow the user to view the operational status of any sensor or system component

3.3.3.4. The system shall display the status of a fully operational sensor or system component using the color green and the word "operational"

3.3.3.5. The system shall display the status of a non-operational sensor or system component using the color red and the word "non-operational"

3.3.3.6. If the ICD defines additional statuses for sensors or system components with which the COP system interacts (as opposed to a NOC/SOC/SD system), then the system shall display those statuses using separate and distinct colors and appropriate words

3.3.3.7. For sensors and system components that can be powered up or down, the system shall display whether that sensor or system component is powered on or off

3.3.3.8. The system shall display the viewshed of a selected sensor on the map

3.3.3.9. The system shall display crosshairs on the map for selected sensors that have single focal points, where the crosshairs match the current focal point of the selected sensor

3.3.3.10. The system shall allow an operator to select a specific point on the map and slew a selected sensor they control, or which is currently uncontrolled, to that location

3.3.4 Map Tools

This section addresses requirements associated with any other tools or features that do not fit appropriately above.

3.3.4.1. The system shall provide access to a unit of measure conversion tool for the operator

3.3.4.2. The system shall provide access to an arithmetic calculator for the operator

3.3.4.3. The system shall provide a compass tool that can be applied to any track or IoI on the map to determine compass heading or bearing

3.3.4.4. The system shall provide a tool that allows the operator to select any two points on the map, and which will display the distance and bearing between the two selected points

3.3.4.5. The system shall allow the operator to define zones on the map by drawing polygons overlayed on the map background

3.3.4.6. The system shall allow the operator to name and save defined zones

3.3.4.7. The system shall allow the operator to configure system alerts based on the movement of IoIs across one or more zones

3.3.4.8. The system shall provide a mechanism to display all tools available for user by the operator

3.3.4.9. The system shall allow the operator to show and hide the display of available tools

3.3.4.10. The system shall allow the operator to select any available tool for use

3.3.4.11. The system shall allow the operator to dismiss any tool in use

3.4 Sensor Command and Control

This section addresses both sensor controls and interactions with sensor-specific displays.

3.4.1 Sensor Control

This section addresses common sensor controls and interactions as well as specific features with which a user can interact for specific sensors (e.g. cameras, radars, loudspeakers, UGS).

3.4.1.1. The system shall allow an operator to select an uncontrolled sensor or system component to control

3.4.1.2. The system shall allow an operator to release a sensor or system component they control

3.4.1.3. The system shall allow a supervisor or system administrator to seize control of a sensor from an operator without having to request control first

3.4.1.4. The system shall notify an operator when someone else has seized control of a sensor they had been controlling, providing the identify of the user to seized control as part of the notification

3.4.1.5. The system shall grant or release control of all sensors or system components mounted on the same PTU at once

3.4.1.6. The system shall allow an operator to access supported configuration settings and capabilities specified in the ICD of a sensor they control

3.4.1.7. The system shall allow the operator to reboot or otherwise restart a sensor or system component

3.4.1.8. The system shall allow the operator to configure a sensor to autoslew to any IoI detected within its surveillance area

3.4.1.9. The system shall allow the operator to configure a sensor to autoslew to an IoI detection from just a specific sensor, which would override a setting to autoslew to any detection in its surveillance area

3.4.1.10. The system shall allow the operator to configure a scan pattern for a specific sensor by defining a ordered points on a map (steps), a linger time for each point, a scan rate between points, and optional start and stop times
3.4.1.11. The system shall allow the operator to assign a name to a scan pattern and save it
3.4.1.12. The system shall allow the operator to retrieve a saved scan pattern
3.4.1.13. The system shall allow the operator to edit the steps of a scan pattern, both by inserting and deleting steps and altering information on existing steps

3.4.2 Sensor Data Displays

This section addresses common sensor data display interactions.

3.4.2.1. The system shall automatically focus any EO/IR or other applicable sensor
3.4.2.2. The system shall allow an operator to manually focus any EO/IR or other applicable sensor they control
3.4.2.3. The system shall allow an operator to zoom in and out on any EO/IR or other applicable sensor they control
3.4.2.4. The system shall allow an operator to adjust the brightness and gain of EO/IR sensors they control
3.4.2.5. The system shall allow an operator to switch between white-hot and black-hot display on IR sensors they control
3.4.2.6. The system shall allow an operator to perform non-uniform correction on IR sensors they control
3.4.2.7. The system shall allow an operator to initiate a laser range finder they control
3.4.2.8. The system shall allow an operator to initiate a laser illuminator they control
3.4.2.9. The system shall allow an operator to set a spotlight they control to on, off, or strobe
3.4.2.10. The system shall allow an operator to turn a loud hailer they control on or off
3.4.2.11. The system shall allow an operator to send a spoken message through a loud hailer they control
3.4.2.12. The system shall allow an operator to play a prerecorded sound file through a loud hailer they control
3.4.2.13. The system shall allow the operator to pan and tilt the devices mounted on a PTU if they control any sensor or system component on that PTU

3.5 Automated Analytics

This section addresses system capabilities in automated detection, identification, classification, and other forms of analysis.

3.5.1 IoI Detection and Track Generation

This section addresses automated capabilities in detecting and tracking IoIs.

3.5.1.1. The system shall automatically determine whether a detected object on the ground is a potential IoI based on the object being at least 1.5 meters high and 0.5 meters wide

3.5.1.2. The system shall automatically determine whether a detected object on the water is a potential IoI based on the object being at least 6.0 meters high and 2.5 meters wide

3.5.1.3. If the detected object is moving slower than 1.5 MPH (threshold - .5 MPH objective), then the system shall not consider it an IoI.

3.5.1.4. If the detected object if moving faster than 45 MPH (threshold – 75 MPH objective), then the system shall not consider it an IoI.

3.5.1.5. If the detected object meets the stated size and speed criteria and can be determined to be human, animal, or conveyance with a confidence rating of 80% or more, then the system shall determine the detected object to be an IoI.

3.5.1.6. The system shall detect IoIs at least 90% (threshold – 95% objective) of the time

3.5.1.7. The system shall limit the determination of false IoIs (i.e. detections that do not meet the size, speed, and identification criteria) to less than 10 % (threshold - 5% objective) of total IoIs displayed.

3.5.1.8. The system shall continuously track the motion of an IoI over time, for as long as it remains within surveillance range

3.5.2 IoI Identification and Classification

This section addresses automated capabilities in identifying and classifying IoIs.

3.5.2.1. The system shall automatically identify an IoI as specifically as possible, based on the following factors:

a) Whether the IoI includes humans, and the number of them in the group

b) Whether the IoI includes animals, and the number of type of them in the group

c) Whether the IoI is primarily conveyance (ground, water, or air), and the number of humans and animals appearing to be in or on that conveyance

d) Equipment or cargo that could represent contraband being carried by the humans, animals, or other conveyance

e) Weapons or other items that could pose threats to agents being carried by the humans, animals, or other conveyance

3.5.2.2. If the detected IoI is human, the system shall further identify any recognizable markings or facial characteristics, and colors during daylight (threshold - and darkness, objective)

3.5.2.3. If the detected IoI is conveyance, the system shall further identify identifying imarkings or information (e.g. vehicle license plate)

3.5.2.4. The system shall assign confidence ratings to its IoI identifications

3.5.2.5. The system shall have the ability to associate the IoI's information when the group of IoI split into smaller groups or individual IoIs.

3.5.2.6. If the system loses track of an IoI, the system shall store the last time of contact with the archived IoI information

3.5.3 Multi-Sensor Correlation and Automation

This section addresses automated capabilities correlating IoIs across sensors.

3.5.3.1. The system shall be able to determine whether IoIs created based on detections from different sensors or systems (e.g. a radar detection and an UGS detection coming in through an external interface) are the same IoI, with 80% confidence.

3.5.3.2. The system shall be able to correlate an IoI detected in one area to an IoI detected at later time in another area (possibly from another sensor feed) based on heading, speed, size, identification, and any other data the system has, with 80% confidence.

3.5.3.3. The system shall ensure all functions that can be performed by a human operator are addressable by automation (e.g. code running as a "virtual agent")

3.6 Data Storage and Retrieval

This section addresses storage, archiving, search, retrieval, file annotation, and export capabilities.

3.6.1 Automated Archiving

This section addresses automated archiving capabilities.

3.6.1.1. The system shall simultaneously record video with metadata and timestamps from every video source within the AoR

3.6.1.2. The system shall, without operator intervention, store all recorded video at the same quality and resolution as viewed by the operator for a minimum of 60 days (threshold - 90 days objective).

3.6.1.3. The system shall store archived data on redundant central storage with snapshot or clone disk-to-disk backup as well as a disaster recovery storage

3.6.1.4. The system shall automatically backup each sensitive information technology (IT) systems, data, and information to the disaster recovery storage unit

3.6.1.5. The system shall allow configurable incremental backup periods, defaulting to daily

3.6.1.6. The system shall allow configurable full backup periods, defaulting to weekly

3.6.1.7. The system shall force a backup before any software modifications are installed

3.6.1.8. The system shall automatically monitor and log data storage system status

3.6.2 Search, Retrieval, and Playback

This section addresses searching archived sensor data, as well as retrieval, playback and annotation.

3.6.2.1. The system shall allow the operator to search for and retrieve

a) Video with associated metadata

b) Individual image frames with associated metadata

c) Radar track history of IoI movements with associated metadata

3.6.2.2. The system shall provide allow the operator playback tools supporting

a) Video with associated metadata.

b) Individual image frames with associated metadata

c) Radar track history of IoI movements with associated metadata

3.6.2.3. The system shall allow the operator to search for stored sensor information by one or more of sensor, date range, and geographical area.

3.6.2.4. The system shall display a list of all archived sensor information that meets the search criteria, along with the sensor name, date ranges, and notes (if the information had been previously annotated).

3.6.2.5. The system shall allow the operator to select a result from the list, which will open an appropriate playback tool

3.6.2.6. The system's video playback tool shall allow the operator to start, stop, pause, and move to a selected point in the video's timeline

3.6.2.7. The system's video playback tool shall allow the operator to view the retrieved video at different frame rates, ranging from at most quarter speed to at least four times normal speed

3.6.2.8. The system's video playback tool shall allow the operator to step through frames one at a time

3.6.2.9. The system's video playback tool shall allow the operator to extract a video clip or a still image from the video.

3.6.2.10. The system's track history tool shall allow the operator to see the track superimposed on the system's map background

3.6.2.11. The system's track history tool shall allow the operator to view the track history with the ability to zoom in, zoom out, and scroll the map

3.6.2.12. The system's track history tool shall allow the operator to identify all information assigned to an IoI at any point along the track

3.6.2.13. The system's playback tools shall allow the operator to view the archived data with no degration in quality

3.6.2.14. The system shall allow the operator to annotate an image in any of the playback tools

3.6.3 Storage and Export

This section addresses data storage and export capabilities.

3.6.3.1. The system shall allow the operator to locally store the

a) Annotated image frames or video clip

b) Full quality video with associated IoI data

3.6.3.2. The system shall enable the operator to edit the associated IoI metadata.

a) The system shall allow the operator to store up to one year the

i. Video and associated metadata with timestamps

ii. Individual image frames and associated metadata with timestamps.

b) The system shall allow the authorized operator to delete

i. Stored video with associated metadata from storage device

ii. Stored individual frames wih associated metadata from storage device

3.6.3.3. The system shall allow the authorized operator to extract video at the same resolution quality as the display on a removable media to support forensic analysis and law enforcement or judicial actions. The removable media are

a) Iron Key

b) Digital Video Discs – Read Only / Digital Video Discs – Read Write (DVD-R/DVD-RW)

3.6.3.4. The system shall allow the authorized operator to export video without loss of video quality in formats compatible with CBP computer resources

a) Video format include MPEG-4 (threshold – H.264 objective)

b) Exported video must be viewable on standard media player like Windows Media Player

3.6.3.5. The system shall allow the operator to store up to one year the

a) Video and associated metadata with timestamps

b) Individual image frames and associated metadata with timestamps.

3.6.3.6. The system shall allow a systems administrator to delete

a) Stored video with associated metadata from a storage device

b) Stored individual frames wih associated metadata from a storage device

4 Nonfunctional Requirements

This section organizes the non-functional requirements for the product. These tend to comprise performance, safety, security, and any number of software quality attributes (often referred to as "ilities").

4.1.1 Performance Description

Performance requirements define how well the system performs certain functions under specific conditions. Latency, throughput, and expected execution time are some examples of performance requirements – generally stated in terms of supporting specific user tasks. Various capacity levels can also be stated as a performance requirement.

Performance requirements need to be considered along with other types of quality attributes as some quality attributes can conflict with one another and require the business to make tradeoffs.

Where a measure of overall execution time is specified in the Joint FRD and applies across both the TPIC and COP, this SRS will allocate half of that time budget to the IST COP.

4.1.2 Performance Requirements

4.1.2.1. The system shall be able to support a minimum of 12 high definition (HD) video feeds at once on a single workstation

4.1.2.2. The system's documentation will define the maximum number of simultaneous HD, standard definition (SD), or other video feeds the system can support

4.1.2.3. The system will need to be able to scale to have a single instance of the system support 37 towers (296 video feeds, 111 PTUs, and as many as 13 operator workstations)

4.1.2.4. For the IST TPIC and COP working together, the roundtrip time from when an operator issues a command to a sensor to when the operator sees the system respond shall not exceed 0.990 seconds (T), or 0.500 seconds (O)

4.1.2.5. The system (i.e., the IST COP, with TPIC responses stubbed out for testing) shall require no more than 0.495 seconds (T), or 0.250 seconds (O) from the time an operator issues a command to when the operator sees the system respond

4.2 Safety

4.2.1 Safety Description

Safety engineering is largely focused on physical systems and their operational environments, and Military Standard 882E (MIL-STD)-882E specified system safety program requirements. However, software does not function independently of the larger system and must be considered in overall system safety engineering efforts. Software supporting safety-critical system functions or controlling safety-critical subsystems requires a higher level of attention and evaluation than most other types of software.

Safety can also address areas of ergonomics or usability that can impact a user's health (though this could also be addressed as a portion of usability under software quality attributes). Examples of requirements in this area would be workstation or user interface design designed to minimize risks of repetitive motion injuries or peripheral specifications to ensure appropriate use.

Safety can also be provided merely by the system performing its innate functions. Border Patrol experience to date provides compelling evidence that IST technology is useful in enhancing agent safety through increased awareness of each tactical situation.

4.2.2 Safety Requirements

4.2.2.1. The system design shall support operations on a workstation where the number of monitors and other devices required for optimal use does not exceed safe personnel reach, access, physical clearance, or visibility dimensions

4.2.2.2. The system design and use of mouse, keyboard, joystick or other devices shall minimize repetetive motions in workload-intensive tasks

4.2.2.3. The provider of the system shall ensure there is an offline training simulation available to operators

4.3 Security

4.3.1 Security Description

Security engineering is generally focused on programmatic activities, though it should reach down into all aspects of a system's development and operations. DHS standard 4300A, the *Sensitive Systems Handbook*, addresses many aspects of security that can be reflected in software requirements. A program's System Security Plan can further define specific activities that may warrant inclusion in a requirements specification.

Many security requirements are functional in nature and have been addressed in Section 3. Examples of these include Identity and Access Management and logging requirements. Non-functional security requirements tend to address the overall state of a system or more general attributes required for a system to respond to attacks. Examples of these include the broad use of encryption technologies or ability to withstand or recover from certain types of attacks.

4.3.2 Security Requirements

4.3.2.1. The system shall protect the confidentiality of sensitive and private (such as Personally Identifiable Information) data during transport and at rest as applicable (laptops or mobile media), by utilizing Advanced Encryption Standard (AES) cryptographic methods that complies with Federal Informaiton Processing Standard (FIPS) 140-2 (as amended).

4.3.2.2. The system shall protect the integrity of sensitive and private (such as Personally Identifiable Information) data during transport and at rest as applicable (laptops or

mobile media), by utilizing AES cryptographic methods that complies with FIPS 140-2 (as amended).

4.3.2.3. The system shall have the validation certificate issued by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program for the AES cryptographics method utilized.

4.3.2.4. The system shall protect against denial of service attacks.

4.3.2.5. The system shall only allow data export to CBP approved universal serial bus devices.

4.4 Software Quality Attributes

4.4.1 Software Quality Attributes Description

There are several types of qualities that can be required in software, which can not adequately be represented as system functions. Among these are availability, reliability, maintainability, portability, extensibility, usability, and more.

Availability tends to be expressed in terms of system or component uptime (or sometimes downtime). Reliability is closely related to availability but tends to be expressed in terms of mean time between failure – sometimes differentiating normal and critical failures – as well as mean time to repair. Maintainability is also related to the previous two quality attributes but tends to describe or constrain when and how maintenance activities can be performed.

System portability requirements are often focused on hardware, but software portability can be expressed in terms of ability to deploy on different operating systems or in different environments. Extensibility is a related principle that often address a system's ability to adapt to changing requirements and new interfaces. These types of requirements tend to address architectural and design concepts like modularity, tight cohesion, and loose coupling, as well as the concept of understandability and inline documentation.

System usability can impact both hardware and software, from ease of learning to ease of use to help subsystems and online documentation. MIL-STD-1472, Human Systems Integration Principles, defines many aspects of usability.

4.4.2 Software Quality Attributes Requirements

4.4.2.1. The System's operational availability shall be equal to or greater than 90% (T), 99% (O)

4.4.2.2. System software failures causing down time shall be resolved within 12 hours

4.4.2.3. The system shall detect and log all component failures, fault alarms, fault alerts, and fault priorities to support external reporting

4.4.2.4. The system shall designed and implemented in accordance with MIL-STD-1472

Appendix A List of Acronyms

Acronym	**Definition**
AES	Advanced Encryption Standard
AoR	Area of Responsibility
ATV	All-Terrain Vehicles
BFT	Blue Force Tracking
BP	Border Patrol
C2	Command and Control
C2CEN	Sector and Station Command and Control Center
CBP	Customs and Border Protection
CCTV	Closed Circuit Television
COP	Common Operating Picture
CVMS	C2 Video Management System
DDM	Degrees, Decimal Minutes
DHS	Department of Homeland Security
DMS	Degree, Minute, Second
DMS	Data Management System
DVD-R	Digital Video Discs-Read Only
eGIS	Enterprise Geospatial Informaiton Services
EO	Electro-Optical
FIPS	Federal Information Processing Standards
FOV	Field of View
FRD	Functional Requirements Document
HD	High Definition
ICAD	Intelligent Computer-Assisted Detection

ICD	Interface Control Document
IFT	Integrated Fixed Tower
IoI	Items of Interest
IR	Infrared
IT	Information Technology
KML	Keyhole Markup Language
LoS	Line of Sight
LOS	Line of Sight
MDP	Maritime Detection Program
MIL-STD	Military Standard
MNS	Mission Need Statement
MPEG	Moving Pictures Experts Group
MSC	Mobile Surveillance Capability
NB-RVSS	Northern Border Remote Video Surveillance System
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
ORD	Operational Requirements Document
PIN	Personal Identification Number
PIV	Personal Identification Verification
PMOD	Program Management Office Directorate
PTU	Pan-Tilt Unit
RVSS	Remote Video Surveillance System
RVSSU	Remote Video Survillance System Upgrade
SBI	Secure Border Initiative
SD	Service Desk
SOC	Security Operations Center

SRS	Software Requirements Specification
SV	System View
TAK	Tactical Assault Kit
TPIC	Towers, Power, Instrumentation, and Communications
TSM	Tracking, Sign-Cutting, and Modeling
UGS	Unattended Ground Sensor
USBP	United States Border Patrol

Appendix B Glossary

Animal – for the purpose of this document, any pack animal or work animal such as donkeys, horses, and mules normally used in carrying humans or cargo

Area of Responsibility (AoR) – the geographical area where border security operations are authorized. USBP formally defines AoRs as the Sector level and Station level. USBP also informally assigns AoRs at the individual agent level according to operational needs

Authorized Operator – user with valid login and appropriate access.

C2 Facility – a room or worksite which supports one or more workstations for RVSS/IFT/MDP, as well as other surveillance systems.

Classify – to assign an appropriate level of threat or importance to an IoI; normally involves viewing an image with sufficient detail to show special facial features, numbers on a license plate, colors, small items of interests (e.g., unconcealed long weapon), etc.

Component –an identifiable part of a larger system that provides a particular function.

Critical Failure - any outage or degradation in one or more components that causes all users on a system instance to be unable to fully execute their mission.

Darkness – outdoor visible light that is low light level ...low to zero light conditions (<1 lux to 0.0001 lux).

Detect – to discover a possible IoI.

EO Camera – daytime camera

False IoI – detection of an IoI that is not human, animal, or conveyance (e.g. trees swaying in the wind).

Field of View (FOV) –- (sometimes called the angle of coverage or angle of view) the angle (in object space) over which objects are recorded on the film or camera in a camera at one time. It depends on two factors, the focal length of the lens and the physical size of the sensor. Since it depends on the camera size, it is not a fixed characteristic of a lens and it can only be stated if the size of the camera it will be used with is known. For a lens used to form a rectangular frame, three fields of view are often given; the horizontal FOV (minimum to maximum camera range), the vertical FOV, and the diagonal FOV.

Group Size –two or more IoIs of the same type (i.e., group of humans, group of animals, or group of conveyances).

Identify – to determine whether an IoI is a human, conveyance, animal, or other object.

Item of Interest (IoI) – humans (on foot, mounted on animals, alone, in groups), animals, and moving conveyances (e.g., ATVs, motorcycles, automobiles, trucks, water craft, drones, ultralight aircraft).

Large Bundle – a carried package of a minimum size of three cubic feet.

Laser Illuminator - A device for enhancing the illumination in a zone of action by irradiating with a laser beam

Latency – system "round trip" latency is defined as the time from C2 user interface joystick control to camera function, and resulting confirmation image back to the C2 user interface monitor. When round-trip latency is 0.990 seconds or better, it is considered "near real time."

Long Weapon – large man-portable firearm (i.e., rifle, shotgun, etc.) that cannot generally be concealed beneath clothing.

Loud Hailer – an intercommunication device intended for limited or private dialogue, direction, collaboration, or announcements. Same as a public address system.

Lux – unit of luminous emittance, measuring luminous flux per unit area. One lux is equal to one lumen per square meter.

Mean Time Between Failure – average time between failures; typically includes all failures without regard to any fault tolerance that may exist.

Mean Time to Repair – the total corrective maintenance time for failures divided by the total number of corrective maintenance actions for failures during a given period of time.

Moving IoI - any IoI having a lateral, closing, or opening rate of motion that equals or exceeds 0.15 meters per second.

Near Real Time – a low-latency time delay of approximately one-half second (i.e., 500 (O) to 990 (T) milliseconds).

Normal Failure – any outage or degradation in one or more components that causes at least one user to be unable to fully execute their mission.

Operational Availability – mission-capable time divided by total time.

Operator – CBP person using the C2 user interface.

Resolution –the accurate reproduction of the scene captured by the imaging device that does not contain noticeable distortion, degradation, noise, or artifacts.

Sensor – a device used to detect and tract IoIs (e.g., camera/scanning).

Site –geographic location of the permanent structure and all components of the platform, sub-platform, and supporting infrastructure.

Spotlight – a strong beam of visible light that can be focused to illuminate a small area.

Video – sequential or continuous streaming of images that appear unbroken to the human eye, typically at specified temporal rates greater than 24 frames/second (Hertz). It does not differentiate between digital and analog.

Viewshed – area of water, land, and/or other environmental element visible from a fixed vantage point.

Appendix C List of References

1. "IEEE Std 830-1998: IEEE Recommended Practice for Software Requirements Specifications", IEEE Computer Society, 20 October 1998, ISBN 0-7381-0332-2
2. U.S Customs and Border Protection, "Joint Functional Requirements Document", Integrated Surveillance Towers (IST), Revision A, 22 August, 2019, Doc # USBP-PMO-IST-00-005001

Appendix D Applicable Specifications, Standards and Handbooks

1. ITU-T Recommendation H.264 (4/2017): "Advanced video coding for generic audiovisual services", ITU-T. April 13, 2017.
2. ITU-T Recommendation H.264.1 (2/2016): "Conformance specification for ITU-T H.264 advanced video coding", ITU-T. February 13, 2016.
3. Department of Homeland Security (DHS) 4300A v12.0: "Sensitive Systems Handbook", November 15, 2015
4. Department of Defense/Intelligence Community/ National System for Geospatial Intelligence (DoD/IC/NSG), , MI STANDARDS PROFILE (MISP), MISP-2018.1
5. MI Standards Board (MISB) MI Sensor Minimum Metadata Set, MISB 0902.4
6. International Telecommunication Union, Telecommunication (ITU-T) standard Ethernet frame transfer and availability performance, ITU-T Y.1563
7. MI Standards Board (MISB) Technical Reference Material, Constructing a MISP Compliant File and Stream, MISB TRM 0909.4
8. National Imagery and Mapping Agency Technical Report, "Department of Defense World Geodetic System 1984", NIMA TR 8350.2 Third Edition
9. Occupational Safety and Health Administration (OSHA) Technical Manual, Chapter 5, "Noise and Hearing Conservation", TED 01-00-015 [TED 1-0.15A]
10. Open Network Video Interface Forum (ONVIF) standard interface for Video Management System, ONVIF, Profile S specification
11. National Health Statistics Reports, Anthropometric Reference Data for Children and Adults: United States, 2003-2006, No 10, NHSR No 10, Oct 2008
12. OTIA Northern and Southern Border Design Reference Mission (DRM) USBP, DRM Version 2.0
13. Environmental Engineering Considerations and Laboratory Tests, MIL-STD-810
14. Interface Standard, Electromagnetic Environmental Effects, MIL-STD-464
15. Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference, MIL-STD-461
16. System Safety Program Requirements, MIL-STD-882
17. Federal Communications Commission (FCC) Electro-Magnetic Compatibility (EMC) Compliance for Un-intentional Radiators, FCC Title 47, CFR Part 15, Class A
18. Federal Information Processing Systems (FIPS) for "certified" devices, FIPS 140-2
19. National Institute of Standards and Technology (NIST) , NIST SP 800-53 Rev 3
20. CBP Physical Security Policy and Procedure Handbook , CBP HB 1400-02B
21. Human Systems Integration (HSI) principles: DOD Design Criteria Standard - Human Engineering, MIL-STD-1472
22. Acquisition Management, CBP DIRECTIVE NO. 5220-041A

23. Department of Defense Interface Standard: Common Warfighting Symbology, MIL-STD-2525C, 17 November 2008

Appendix E Notional Architecture Models

As part of a systems engineering trade study PMOD commissioned HSSEDI to perform evaluating alternate acquisition paths for acquiring the IST COP system, HSSEDI developed a COP system notional functional architecture and delivered as separate document [1]. Those notional functional architecture model is attached here for reference. This architecture focuses on core services required for a COP system. The functions identified in this notional architecture were inturn derived from this SRS document.

Figure 2 below depicts the internal resource flow for the IST COP system. This architecture view is the detailed version of Figure 1. Which follow the design patterns of Department of Defense Architecture Framework (DoDAF) System View (SV) 2, systems internal resource flow description; and SV-4, systems functionality description. These views roughly correspond with Federal Enterprise Architecture Framework (FEAF) application communication diagrams (A-1) and data flow diagrams (D-4).

Figure 3 through Figure 9 depicts a second-level decomposition of the first-level IST COP functions with descriptions of each function. In the diagrams, functions that are depicted in a grey color are considered optional, as the function they provide is either a desired capability that is not yet a requirement for the system or a capability that can easily be allocated to an external component.

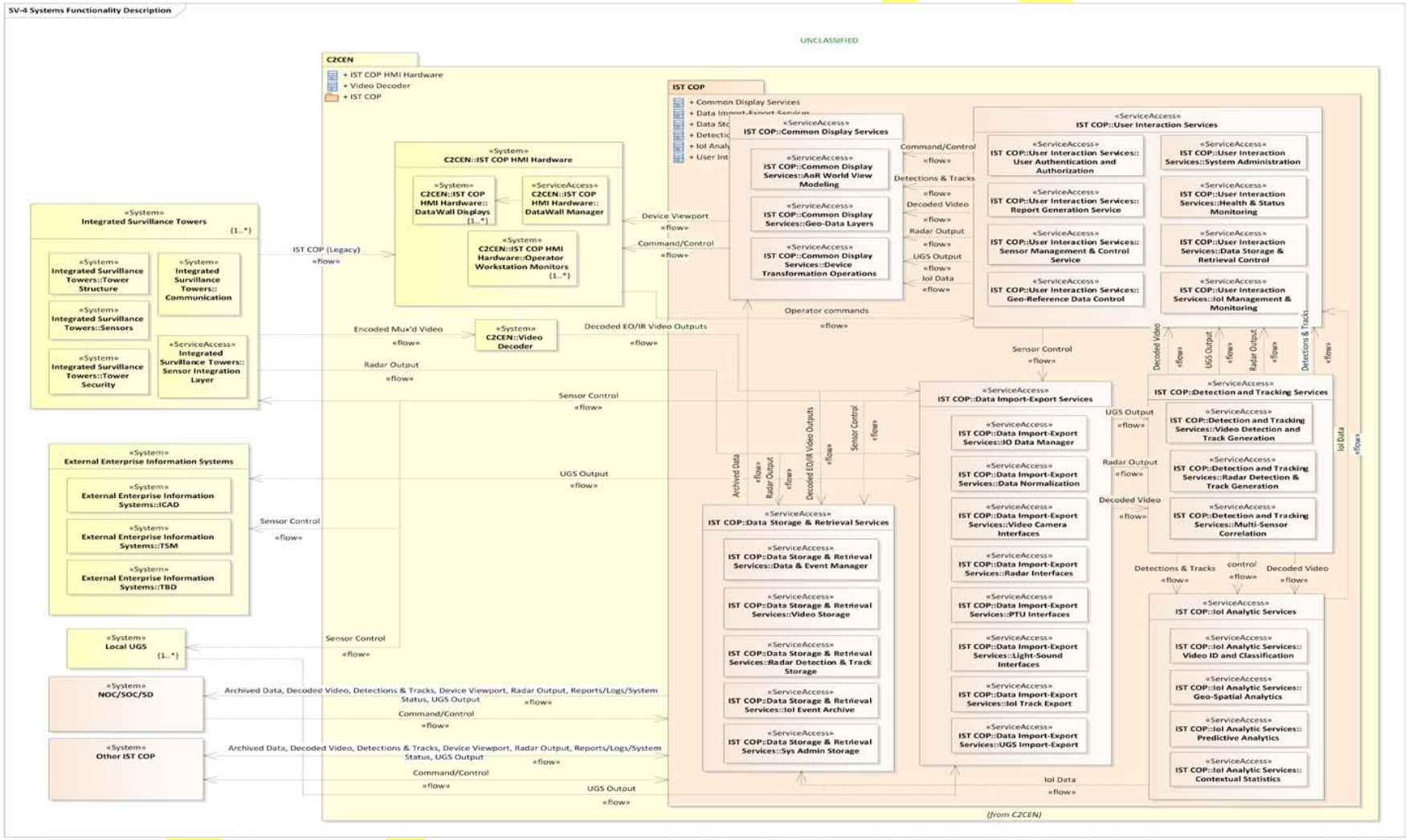

Figure 2. IST COP System Internal Resource Flow Diagram

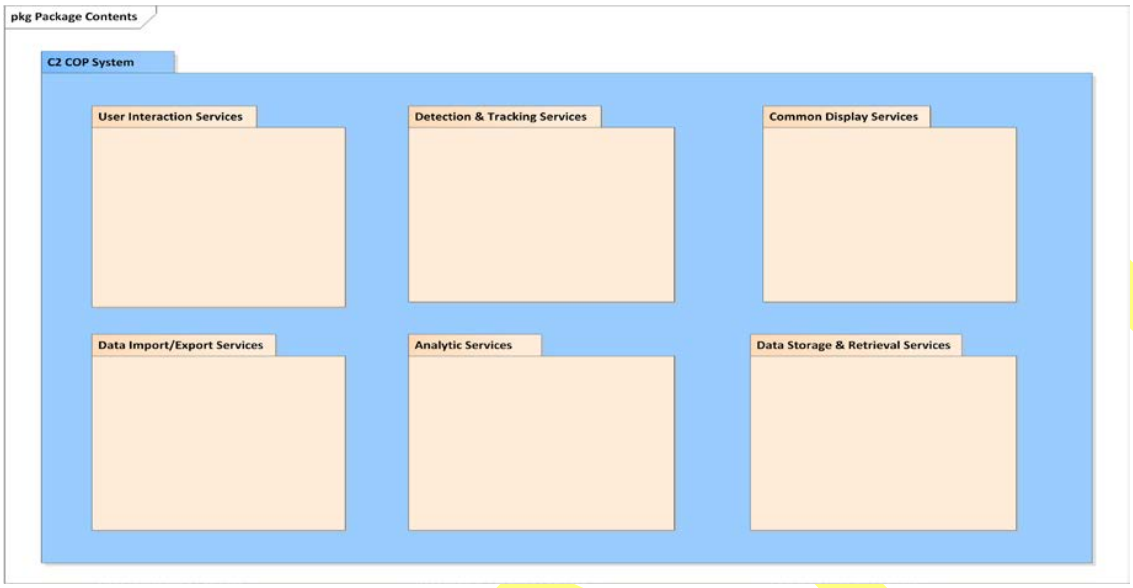

Figure 3. IST COP First Level System Functions

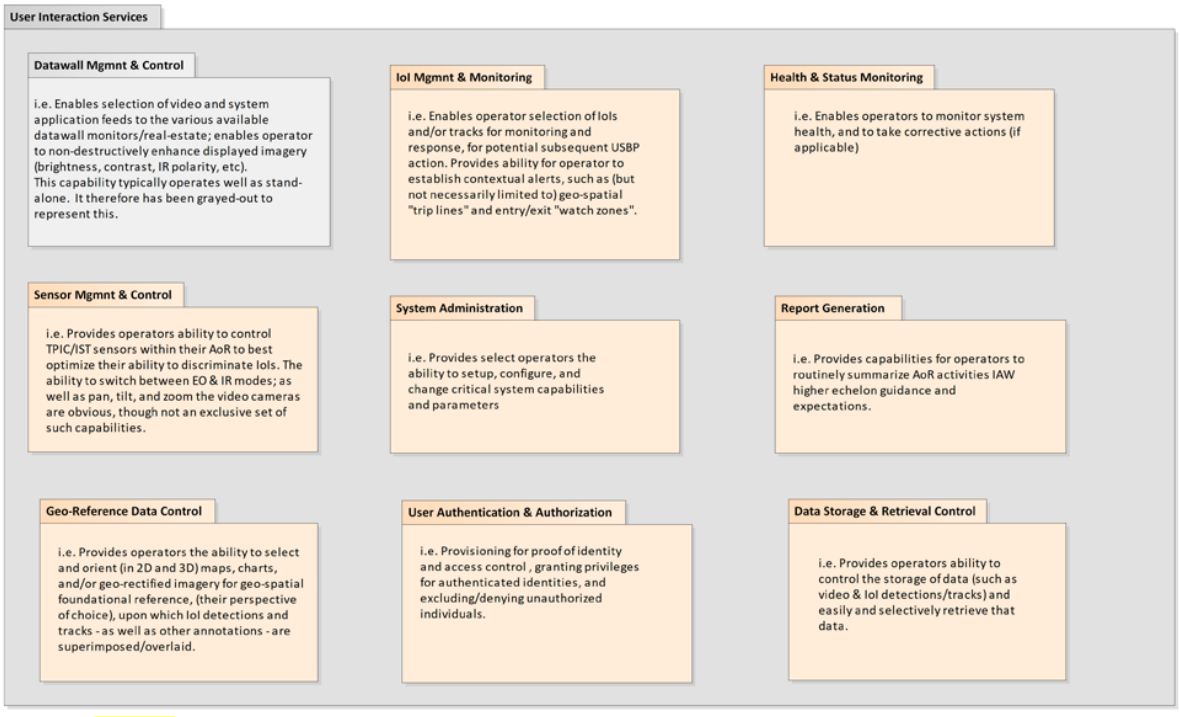

Figure 4. IST COP Second Level Functional Description for User Interaction Services

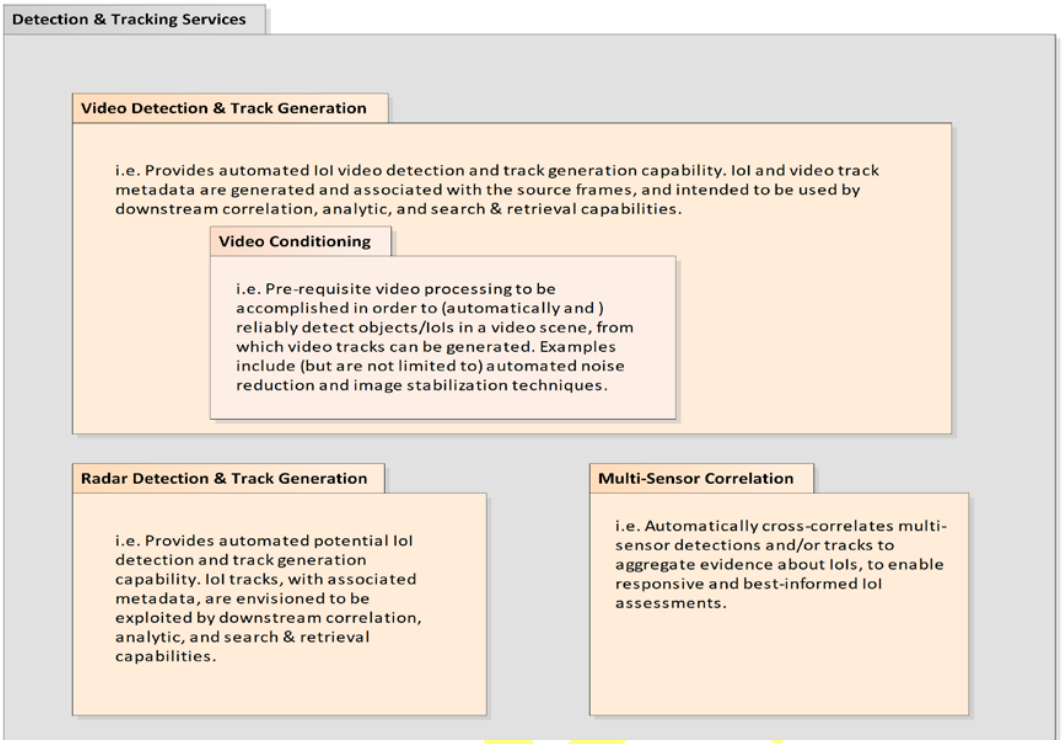

Figure 5. IST COP Second Level Functional Description for Detection and Tracking Services

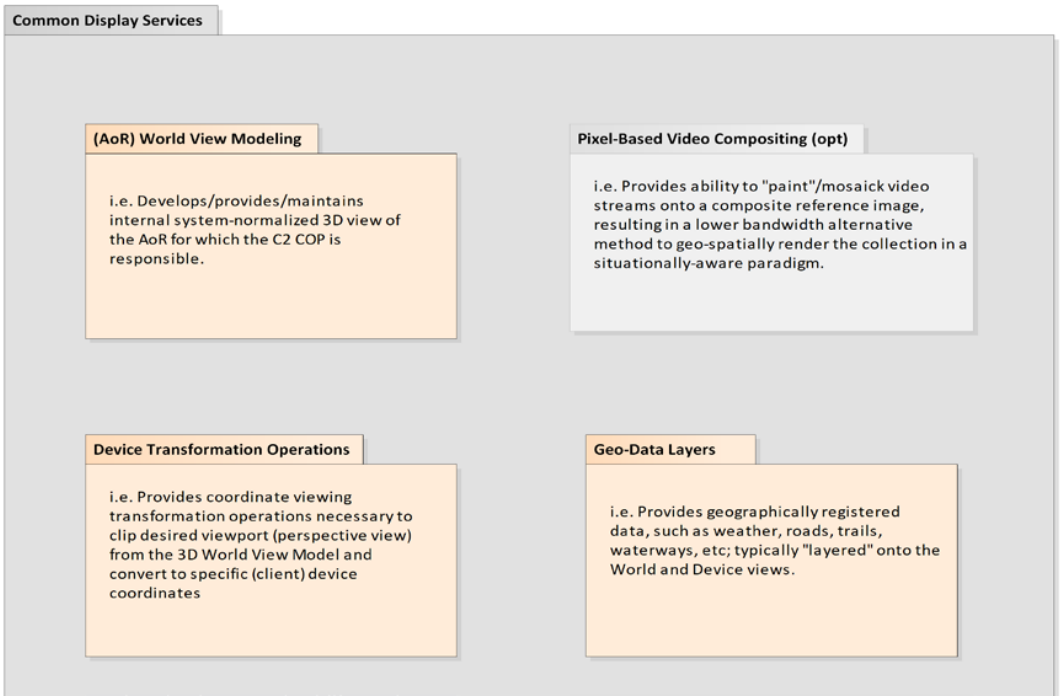

Figure 6. IST COP Second Level Functional Description for Common Display Services

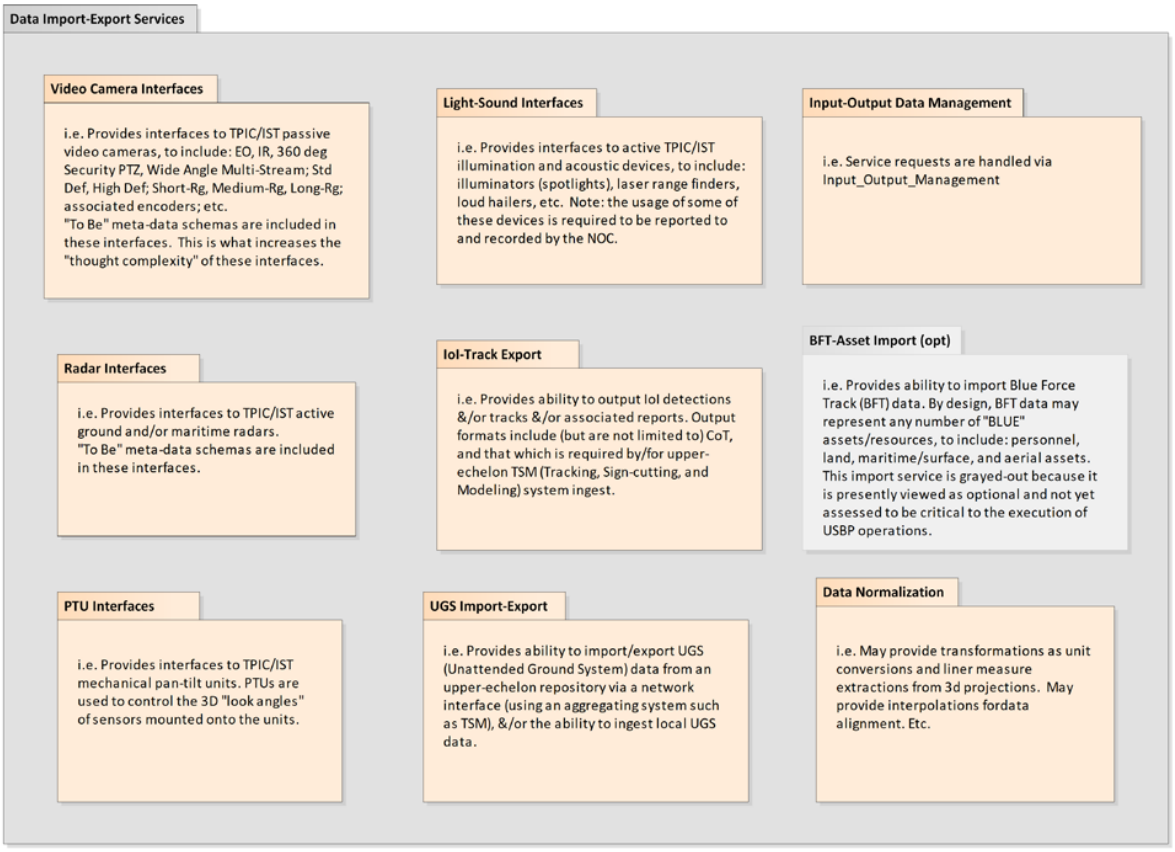

Figure 7. IST COP Second Level Functional Description for Data Import-Export Services

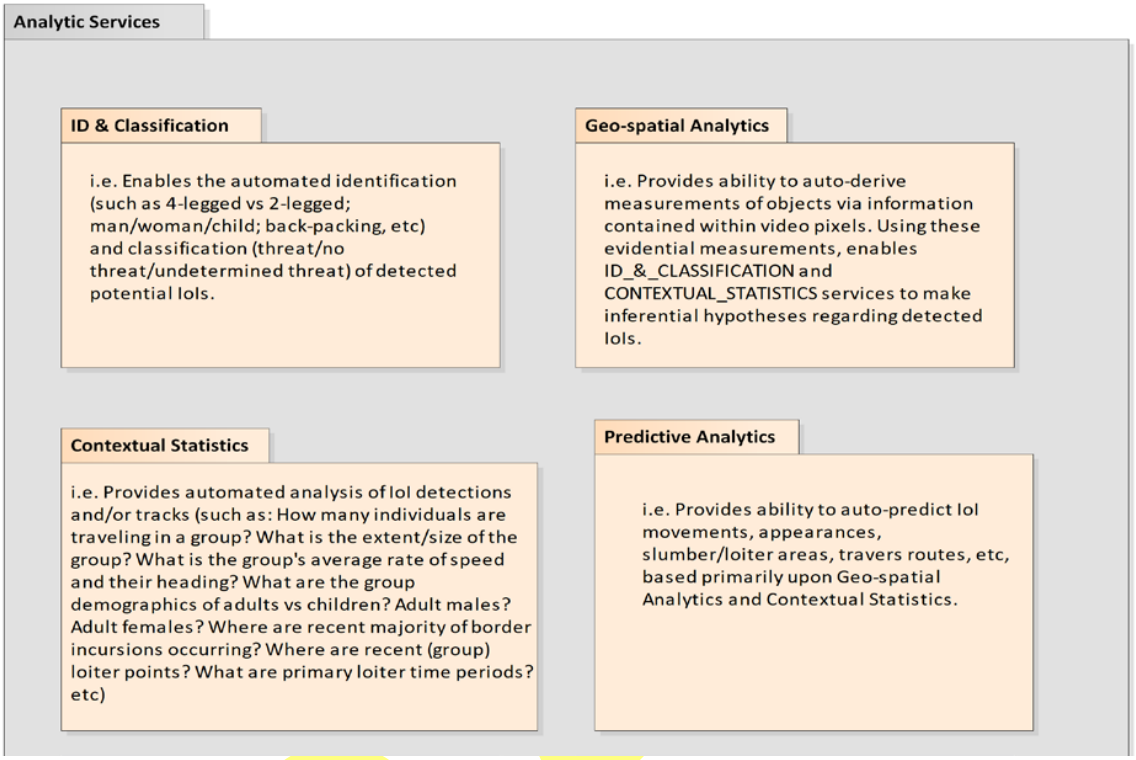

Figure 8: IST COP Second Level Functional Description for Analytic Services

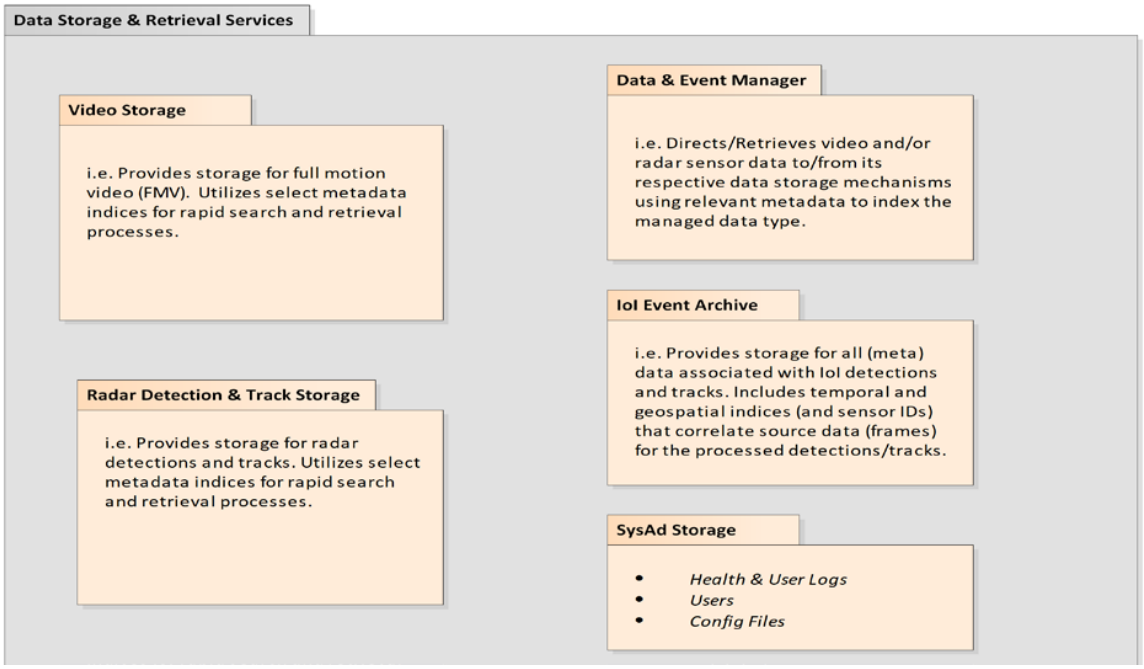

Figure 9: IST COP Second Level Functional Description for Data Storage and Retrieval Services

Appendix F Traceability

Requirements will be traced to parent requirements in the JFRD, Rev A, dated 22 August 2019.

SRS Reqt ID	Parent Reqt Source & ID	Verification Method